Deputy Assistant Secretary of Defense for Cyber, Identity, and Information Assurance Strategy

August 2009

The Office of the Assistant Secretary of Defense
for
Networks and Information Integration / DoD Chief Information Officer

# Report Documentation Page	*Form Approved* *OMB No. 0704-0188*

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE **AUG 2009**	2. REPORT TYPE	3. DATES COVERED **00-00-2009 to 00-00-2009**

4. TITLE AND SUBTITLE **Deputy Assistant Secretary of Defense for Cyber, Identity, and Information Assurance Strategy**	5a. CONTRACT NUMBER
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Office of the Assistant Secretary of Defense ,for Networks and Information Integration / DoD Chief Information Officer,Washington,DC,20301**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**32**	

THIS PAGE INTENTIONALLY LEFT BLANK

Executive Message

The United States, its friends and allies face a world of complex challenges and great opportunities. Nowhere are those challenges and opportunities more apparent than in cyberspace. With information and information technology assets distributed over a vast and wide-ranging enterprise and with diverse domestic and international partners actively participating in DoD missions, we know that we cannot execute operations without the Global Information Grid (GIG). The GIG is where business goods and services are coordinated; where medical information resides; where intelligence data is fused; where weapons platforms are designed, built and maintained; where commanders plan operations and command and control forces; and where training, readiness, and morale and welfare are sustained. Maintaining freedom of action in cyberspace is critical to the Department and to the Nation.

Therefore, the Department is focused on building and operating the GIG as a joint global enterprise. This enterprise network approach, coupled with skilled users, defenders, and first-responders, and in partnership with the intelligence and homeland security communities and the private sector, will allow us to more readily identify and respond to cyber degradation or attack -- and still accomplish our missions.

This strategy lays out our vision and goals for cyber, identity and information assurance. It builds on insights gained and lessons learned, and it represents the distillation of valuable experience from throughout the Department. It also emphasizes the critical role our partners play – within the U.S. government, the private sector, and internationally – in achieving our common goals.

The complex cybersecurity issues facing the Department and the Nation are fundamental and long term. This strategy is a blueprint to succeed in years to come.

Robert F. Lentz
Deputy Assistant Secretary of Defense for
Cyber, Identity and Information Assurance

THIS PAGE INTENTIONALLY LEFT BLANK

Executive Summary

This document serves as the overarching strategy for the office of the Deputy Assistant Secretary of Defense for Cyber, Identity and Information Assurance (CIIA). It is aimed at influencing the DoD Components and supports all business, warfighting, and intelligence missions across all Tier 1 Joint Capability Areas, with specific focus on the computer network defense tasks in Force Application, the information assurance (IA) tasks in Net Centric, and related information management tasks in Corporate Management and Support.

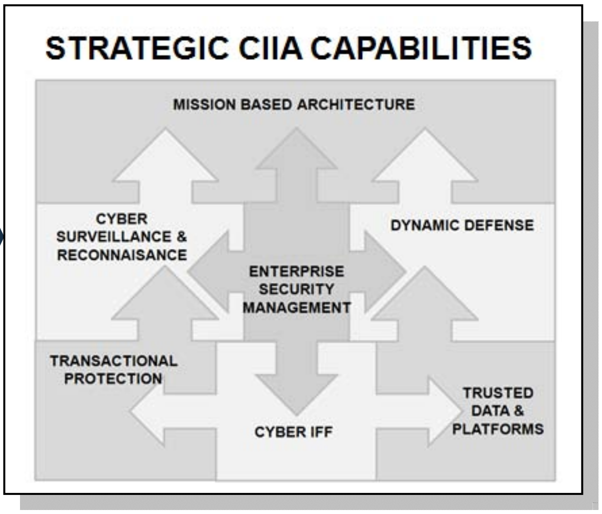
It sets forth to support the DoD vision of freedom of action in cyberspace, where:

- DoD missions and operations continue under any cyber situation or condition.
- The cyber components of DoD weapons systems and other defense platforms perform only as expected.
- DoD cyber assets collectively, consistently, and effectively act in their own defense.
- The Department has ready access to its information and command and control channels, and its adversaries do not.
- The Department of Defense information enterprise securely and seamlessly extends to mission partners.

T o accomplish this vision four goals have been established that collectively describe an integrated approach for focusing near-term activity and aligning long-term investment, and it identifies a unified set of strategic CIIA capabilities that emerge from the activities described in the goals.

GOALS

1. Organize for unity of purpose and speed of action.
2. Enable secure mission driven access to information and services.
3. Anticipate and prevent successful attacks on data and networks.
4. Prepare for and operate through cyber degradation or attack.


STRATEGIC CIIA CAPABILITIES
MISSION BASED ARCHITECTURE
CYBER SURVEILLANCE & RECONNAISANCE
DYNAMIC DEFENSE
ENTERPRISE SECURITY MANAGEMENT
TRANSACTIONAL PROTECTION
CYBER IFF
TRUSTED DATA & PLATFORMS

Implementation details for this strategy will be published via a separate plan, along with an enterprise schedule and enterprise metrics. The GIG IA Portfolio (GIAP) supports CIIA in the Department's decision processes (Joint Capabilities Integration Development System (JCIDS); Planning, Programming and Budget Execution (PPBE); and Defense Acquisition System (DAS)) and adjusts the portfolio over time to reflect the Department's priorities and outcomes.

THIS PAGE INTENTIONALLY LEFT BLANK

Table of Contents

I. Introduction

The Department of Defense (DoD) issued its first information assurance (IA) strategy in 2004. Much has changed since then. We have witnessed a significant increase in threat, with the advent of orchestrated cyber attacks against national governments; seen focused campaigns to target and exfiltrate scientific and technical information of military significance from industry and academia; and operationally been at the vortex of a steady increase in sophisticated attempts to penetrate DoD networks and information systems.

Our emphasis has also increased. During the past five years the Department has:

- Under Presidential leadership, joined forces with other federal agencies in a comprehensive national cybersecurity initiative to secure government networks, protect against constant intrusion attempts, and anticipate future threats.
- Developed a DoD Information Management/Information Technology (IM/IT) Strategic Plan for achieving information advantage.
- Recognized cyberspace as a global domain within the information enterprise, developed a National Military Strategy for Cyberspace Operations (NMS-CO), embraced a Network Operations (NetOps) construct for operating and defending the Global Information Grid (GIG), and, under United States Strategic Command (USSTRATCOM), integrated NetOps with other cyber operations and established a Sub-unified US Cyber Command (USCYBERCOM).

> The U.S. Government defines ***cybersecurity*** as "prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and non-repudiation" (NSPD 54/HSPD 23).

- Developed the IA Component of the GIG Integrated Architecture and strategies and programs for delivering key identity and IA capabilities as enterprise services.
- Partnered with the Director for National Intelligence (DNI) to establish the Unified Cross Domain Management Office (UCDMO) to synchronize and accelerate the availability of assured information sharing solutions.
- Established a cybersecurity program in partnership with the Defense Industrial Base (DIB) to protect unclassified information relevant to Defense-related research and development.
- Embraced a capabilities portfolio management (CPM) construct that includes Net-Centric as a Tier 1 Joint Capability Area (JCA) and IA as a Tier 2 capability area within the Net-Centric JCA.
- Established supply chain risk management as a core Department program and a National priority.

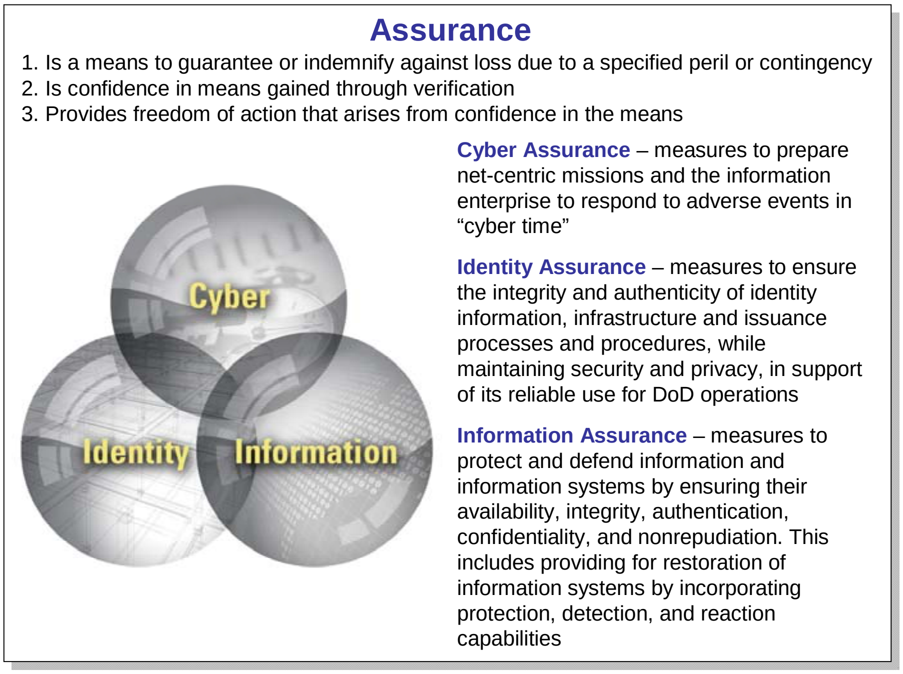
However, our adversaries remain highly motivated to see our information, subvert our command and control channels, and deny us use of our information and communications infrastructure. They are:

- Persistent, and growing in capability and motivation.
- Taking advantage of the greater access and concealment opportunities in the globally interconnected cyber environment.
- Taking advantage of global supply chains to move attacks forward in the information and communications technology (ICT) lifecycle.

A further increase in emphasis is imperative to protect and defend the Department against current and future threats, accelerate the transformation to a net-centric enterprise with assured information access, ensure the survivability of GIG-dependent missions, and ensure the integrity of weapons systems and other defense platforms with embedded processors and controllers.

II. Purpose

This document serves as the overarching strategy for the office of the Deputy Assistant Secretary of Defense for Cyber, Identity and Information Assurance (CIIA), and provides the common vision and goals that guide and integrate the Department's many CIIA initiatives and investments. It is intended to influence the CIIA strategy for the Office of the Secretary of Defense, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Military Departments, the Office of the Inspector General of the DoD, the Defense Agencies, the DoD Field Activities, and all other organizational entities in the DoD.



Assurance

1. Is a means to guarantee or indemnify against loss due to a specified peril or contingency
2. Is confidence in means gained through verification
3. Provides freedom of action that arises from confidence in the means

Cyber Assurance – measures to prepare net-centric missions and the information enterprise to respond to adverse events in "cyber time"

Identity Assurance – measures to ensure the integrity and authenticity of identity information, infrastructure and issuance processes and procedures, while maintaining security and privacy, in support of its reliable use for DoD operations

Information Assurance – measures to protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities

Figure 1. Cyber, Identity, and Information Assurance

Its contents should be referenced and incorporated into DoD Component and CPM) plans that impact CIIA capabilities. It updates and replaces the DoD 2004 Information Assurance Strategic Plan and all interim updates, and reinforces the critical contribution of the CIIA community in making DoD networks, information and information technologies secure, available, and sound for purpose. It implements national cybersecurity policy and strategy, helps shape National and global cybersecurity markets and technology pipelines, and it supports the full IM/IT life cycle across all defense business, intelligence and warfighting missions and operations, as illustrated in Figure 2.

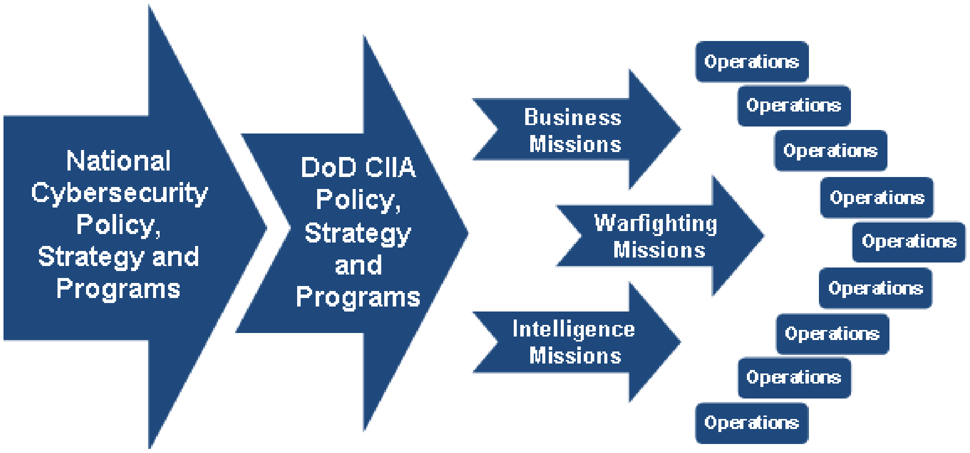


Figure 2. DoD CIIA Strategy Implements National Policy and Strategy and Supports all DoD Missions and Operations

Mission success in all nine Tier 1 JCAs (Force Application, Command and Control, Battlespace Awareness, Net Centric, Building Partnerships, Protection, Logistics, Force Support, and Corporate Management and Support) relies on timely availability of trustworthy information and information services. This strategy enables mission accomplishment across all JCAs and specifically addresses computer network defense tasks in Force Application, IA tasks in Net Centric and related Information Management tasks in Corporate Management and Support.

The Department's cyber assets are assured by initiatives that span the DOTMLPF[1] spectrum and extend across every DoD organization, mission, and system. This strategy informs and supports the Department's decision processes: Joint Capabilities Integration Development System (JCIDS), Planning, Programming, Budgeting, and Execution (PPBE), and Defense Acquisition System (DAS). It provides a framework for integration across workforce development, architecture and engineering, portfolio management, acquisition, operations, and assessments and evaluations.

[1] Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel and Facilities

III. Vision and Scope

The DoD vision is freedom of action in cyberspace, where:

- DoD missions and operations continue under any cyber situation or condition.
- The cyber components of DoD weapons systems and other defense platforms perform only as expected.
- DoD cyber assets collectively, consistently, and effectively act in their own defense.
- The Department has ready access to its information and command and control channels, and its adversaries do not.
- The Defense information enterprise securely and seamlessly extends to mission partners.

There are many challenges to realizing and sustaining this vision; among them:

- **Being united**. Cyber assets are planned, resourced, acquired, deployed, and operated across a multiplicity of missions, organizations, acquisitions, and systems-of-systems, often without thought for their role in keeping the enterprise agile or sustainable.

- **Being prepared**. Today, adversaries are collecting information on and about DoD networks to understand our capabilities. In the future, conventional and irregular warfare will include cyber attacks to disrupt, co-opt, manipulate, or destroy DoD networks and information.

- **Being aware**. Dependence on cyber capabilities is pervasive but often unacknowledged.

- **Countering cyber asymmetry**. Cyber attacks can be launched with low risk, a low threshold of investment in capability, from a distance, and with anonymity. Yet, cyber attacks can deliver significant value to the attacker and have high consequences to those being attacked.

- **Predicting cyber effects**. Cyber event damage can propagate along many different yet changing vectors, and may be non-localized.

To realize all aspects of the vision, overcome these and other challenges, and effectively support all Tier 1 JCAs, CIIA activities must be synchronized, and investments must favor those that deliver CIIA capability in more than one area. All CIIA capabilities must work together to improve confidence and speed of action.

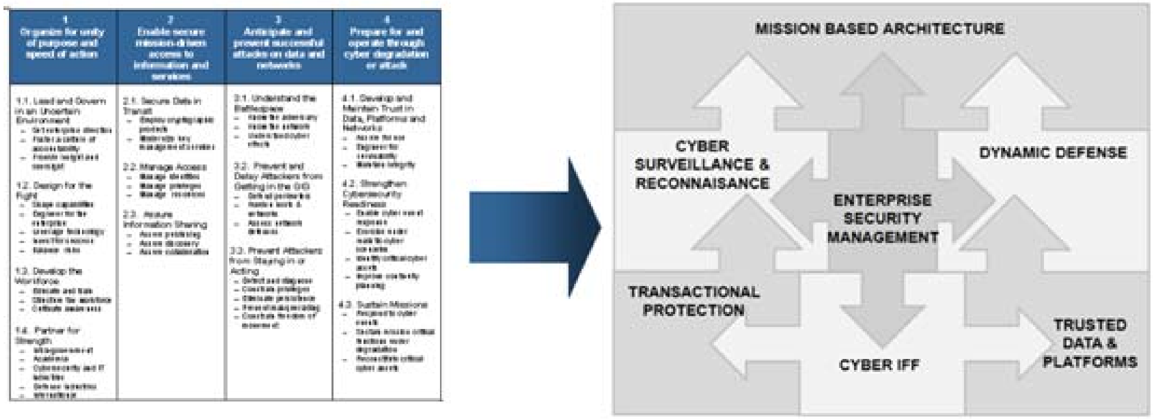
This strategy lays out four goals for creating and sustaining effective CIIA capabilities, consistent implementation, and coordinated responses. Collectively, these goals describe an integrated approach for improving level of confidence and speed of action. They help organize and focus CIIA activities in the Department immediately, and provide the long-term investment framework for realizing the Department vision.

Table 1 provides an overview of the activities within each goal. They are presented as a hierarchy for ease of reading and for organizing work and investments; however, over time, focused individual efforts within the goals create the unified set of strategic capabilities summarized in Table 2 and discussed in Appendix B.

Table 1. Overview of CIIA Goals

1 Organize for unity of purpose and speed of action	2 Enable secure mission-driven access to information and services	3 Anticipate and prevent successful attacks on data and networks	4 Prepare for and operate through cyber degradation or attack
1.1. Lead and Govern in an Uncertain Environment – Set enterprise direction – Foster a culture of accountability – Provide insight and oversight **1.2. Design for the Fight** – Shape capabilities – Engineer for the enterprise – Leverage technology – Invest for success – Balance risks **1.3. Develop the Workforce** – Educate and train – Structure the workforce – Cultivate awareness **1.4. Partner for Strength** – Intra-government – Academia – Cybersecurity and IT industries – Defense industries – International	**2.1. Secure Data in Transit** – Employ cryptographic products – Modernize key-management services **2.2. Manage Access** – Manage identity credentials – Manage privileges – Manage resources **2.3. Assure Information Sharing** – Assure publishing – Assure discovery – Assure collaboration	**3.1. Understand the Battlespace** – Know the adversary – Know the network – Understand cyber effects **3.2. Prevent and Delay Attackers from Getting in the GIG** – Defend perimeters – Harden hosts & networks – Assess network defenses **3.3. Prevent Attackers from Staying in or Acting** – Detect and diagnose – Constrain privileges – Eliminate persistence – Prevent masquerading – Constrain freedom of movement	**4.1. Develop and Maintain Trust in Data, Platforms and Networks** – Assure for use – Engineer for survivability – Maintain integrity **4.2. Strengthen Cybersecurity Readiness** – Enable cyber event response – Exercise under realistic cyber scenarios – Identify critical cyber assets – Improve continuity planning **4.3. Sustain Missions** – Respond to cyber events – Sustain mission critical functions under degradation – Reconstitute critical cyber assets

Table 2. Strategic CIIA Capabilities Emerge from Activities of Goals 1-4 and Build on One Another


1
Organize for unity of purpose and speed of action
2
Enable secure mission-driven access to information and services
3
Anticipate and prevent successful attacks on data and networks
4
Prepare for and operate through cyber degradation or attack
1.1. Lead and Govern in an Uncertain Environment
1.2. Design for the Fight
1.3. Develop the Workforce
1.4. Partner for Strength
2.1. Secure Data in Transit
2.2 Manage Access
2.3. Assure Information Sharing
3.1. Understand the Battlespace
3.2. Prevent and Delay Attackers from Getting in the GIG
3.3. Prevent Attackers from Staying in or Acting
4.1. Develop and Maintain Trust in Data, Platforms and Networks
4.2. Strengthen Cybersecurity Readiness
4.3. Sustain Missions
MISSION BASED ARCHITECTURE
CYBER SURVEILLANCE & RECONNAISANCE
DYNAMIC DEFENSE
ENTERPRISE SECURITY MANAGEMENT
TRANSACTIONAL PROTECTION
TRUSTED DATA & PLATFORMS
CYBER IFF

Described in Ascending Order:

Transactional Protection

What: Granular end-to-end security controls for each information transaction in a variable trust environment.

Why: Provides privacy and protects against interruption, corruption or non-repudiation of information transactions.

Cyber Identification Friend-or-Foe (IFF)

What: Universal cyber IFF for all person (individuals, roles, COIs, organizations) and all non-person (devices, platforms, data, services, systems, networks) entities in the GIG and its extensions to mission partners.

Why: Enables distinction among friendly, neutral, and adversary cyber entities and ensures friendly cyber entities are visible, trackable, and addressable for management and control.

Trusted Data and Platforms

What: Robust integrity mechanisms protecting Defense data and embedded within GIG and weapons system components and maintained over their life cycle.

Why: Protects ICT components against attacks during manufacture or distribution (i.e., "supply chain") and provides early warning and automated mitigation of data or platform degradation.

Cyber Surveillance & Reconnaissance

What: Technologies and processes to persistently observe GIG user, asset, and network behavior and examine their characteristics or configuration in order to detect anomalies, misuse, or unauthorized activity.

Why: Provides knowledge and situational awareness of the GIG.

Enterprise Security Management

What: Integrated enterprise services for all security functions (e.g., identity, credential, attribute, policy, privilege, authentication, configuration, audit, and cryptologic key management).

Why: Efficient, effective, and consistent implementation of security functions across the enterprise plus ability to rapidly respond to changing needs.

Dynamic Defense

What: Enterprise security management infrastructure linked to and alerted by extended cyber sensor networks.

Why: Provides warning and means to respond beyond the GIG.

Mission Based Architecture

What: Networks, services, and data organized and optimized for mission availability.

Why: Lessening of security technology constraints over time along with heightened mission awareness of cyber risk enables better alignment of the information enterprise with mission needs.

IV. GOALS

For each goal, this section provides the rationale, the expected outcomes, the direction of change the goal is intended to enable, and the approach for achieving the goal.

Goal 1. Organize for unity of purpose and speed of action

Rationale: In response to 21st century global security concerns, the Department has adopted a net-centric operations (NCO) model. In a NCO model, people, services, and platforms can discover one another and connect to form new capabilities or teams without being constrained by geographic, organizational, or technical barriers, and they can work together to achieve shared ends. Cybersecurity is a global security concern, and CIIA needs to be net-centric. This means that CIIA capabilities are designed, organized and managed such that they can work together in any combination that events demand, they maintain an expected level of readiness, and all required CIIA assets can be brought to bear in a rapid and flexible manner to meet new or changing mission needs. Further, this means that DoD CIIA capabilities can dynamically work with the CIIA capabilities of the U.S. Government and mission partners to support shared objectives, and that requirements and acquisition processes account for ICT product and service provider risk.

Outcomes:

- All DoD organizations and communities of practice understand the extended CIIA community and each knows its role.
- The Department has the willingness and the mechanisms to align its culture and conduct to changing CIIA demands.
- The Department effectively leverages its decision processes (JCIDS, PPBE, and DAS), the global marketplace, workforce development mechanisms, and emerging technologies to create and deliver the right CIIA capabilities on the right timelines.
- The DoD CIIA workforce is unmatched in skills and expertise.
- The Department can count on its partners, and its partners can count on it.

Direction of Change:

From	To
Security technology constrains mission.	Security enables mission and user needs.
Risk calculations and decisions are local.	Risk calculations and decisions are a balance of enterprise and local considerations.
Governance is stove-piped.	The enterprise provides leadership in the face of uncertainty and actively manages risk.
IA capabilities are primarily local in scope, and they emerge from many independently designed networks and information systems.	CIIA capabilities are purposefully designed and synchronized through enterprise architecture, enterprise systems engineering, a focused technology pipeline, and active portfolio management.
IA is an IT specialty.	CIIA is integral to all missions and operations.
IA is an "other duty as assigned."	CIIA is a profession or military occupational specialty.
DoD acting alone.	DoD in partnership with other federal agencies, industry, academia, and mission partners.

Table 3. Direction of Change Enabled by Goal 1

Strategy Elements:

1.1. **Lead and Govern in an Uncertain Environment**. Provide vision and follow-through.

1.1.1. ***Set Enterprise Direction***. Establish and communicate priorities and objectives, principles, policies, standards, and performance measures.

1.1.2. ***Foster a Culture of Accountability***. Align internal processes, tighten accountability and inform, make, and follow through on decisions with implications for the cyber protection and defense of the enterprise.

1.1.3. ***Provide Insight and Oversight***. Measure, review, monitor, supervise, and remediate to ensure coordinated and consistent CIIA implementation across all organizations without impeding local missions.

1.2. **Design for the Fight**. Deliver the right capabilities on the right time line. Synchronize and integrate capabilities across the enterprise.

1.2.1. ***Shape Capabilities***. Continually work with all mission areas, Capability Managers, Program Executive Officers (PEOs) and Program Management Offices (PMOs), communities of practice, and GIG operators and users to explain CIIA capabilities and understand CIIA needs.

1.2.2. ***Engineer for the Enterprise***. Partner with enterprise architecture and systems engineering entities and provide the blueprint for how needed capabilities are to be delivered and interact.

1.2.3. ***Leverage Technology***. Continually assess technology needs, performance, availability and sources, and identify effective ways to achieve strategic objectives.

1.2.4. ***Invest for Success***. Continually align programs, initiatives, and activities with enterprise priorities and warfighter requirements.

1.2.5. ***Balance Risks***. Provide approaches and enterprise decision processes for understanding and managing risk to operations, assets, individuals, organizations and the Nation arising from the incorporation of information and communications technology into mission and business processes.

1.3. **Develop the Workforce**. Provide a continuum of learning activities from basic literacy to advanced specialties, recruit and retain highly qualified professionals in needed positions, and keep workforce capabilities current in the face of constant change.

1.3.1. ***Educate and Train***. Partner with academia to train and sustain a workforce with the depth and breadth of skill and expertise to anticipate, engineer for, and defend against sophisticated cyber adversaries.

1.3.2. ***Structure the Workforce***. Define operational skills and specialties, determine organizational needs and put the right number of jobs in the right places. Put the right people in the right jobs.

1.3.3. ***Cultivate Awareness***. Enlist all users and decision makers in support for CIIA objectives.

1.4. **Partner for Strength**. Leverage the unique capabilities of a wide set of partners to create advanced CIIA capabilities.

1.4.1. ***Intra-Government***. Support and benefit from CIIA-related programs and initiatives throughout the US government.

1.4.2. ***Academia***. Help build future generations of CIIA professionals.

1.4.3. ***Cybersecurity and IT Industries***. Expand technical relationships with critical providers.

1.4.4. ***Defense industries***. Partner with members of the Defense Industrial Base to strengthen cybersecurity of defense-related research and development.

1.4.5. ***International***. Enhance global cybersecurity situational awareness and build partner capacity.

Goal 2. Enable secure mission-driven access to information and services

Rationale: The defense enterprise is global, and its missions and mission partners are dynamic and diverse. Information needs to flow to all corners of the enterprise and access to information and services needs to be driven by and be responsive to mission needs. Defense information is a high value target and it needs to be protected from the many adversaries who are motivated to steal it. The enterprise needs to have visibility and control of all its information assets, and the management channels that allocate information resources to missions need to be secure. Cryptography creates a hard outer shell to protect DoD information flows from interception or disruption. Identity services provide strong, high confidence credentials for all entities (e.g., individuals, roles, organizations, communities of interest (COIs), devices, services, platforms). More granular controls allocate resources and mediate transactions to keep the enterprise from being "soft on the inside."

Outcomes:

- DoD information is not disclosed to adversaries.
- DoD information and information resources are visible and securely accessible to all who need them.
- The information enterprise can quickly adjust to changing mission needs.
- Secure collaboration within DoD and with mission partners is seamless and agile.

Direction of change:

From	To
System High.	Variable Trust.
All users are friendly persons.	Every person and non-person entity in the information enterprise has a unique digital identity; adversary and neutral forces are identified too.
Access mechanisms are different for every application.	Enterprise services decouple identity and privilege management from applications.
Policy is a document that is updated every three years.	Policy is digitally instantiated in the information enterprise and can be dynamically adapted to mission needs.
Network and resource connection (access) is granted on the basis of human inspection. Once connected, always connected.	Connection is "machine-adjudicated" on the basis of recognized identity credentials, authorization, and satisfaction of security/risk criteria. Continued connection may be conditional upon sustainment of security/risk criteria.
Crypto devices are pre-placed for connectivity.	Crypto is an enterprise service with over-the-net-keying (OTNK). Where appropriate, connections with mission partners are simplified through adoption of commercial standards and products.
Provisioning practices assume that all users are fixed.	Unanticipated users are recognized through federation agreements or they are provisioned rapidly, and COIs are constructed on the fly.
Information is physically separated by security level.	Information is logically separated.

Table 4. Direction of Change Enabled by Goal 2

Strategy Elements:

2.1. **Secure Data-in-Transit**. Enable private information flows through robust, ubiquitous cryptographic services. (Note. Protection for data-at-rest is under 3.3 and 4.1)

2.1.1. ***Employ Cryptographic Products***. Incorporate the means to make information flows private, confidential, and protected against unauthorized modification or corruption. Make cryptographic products easier to use, more affordable, and more available to mission partners.

2.1.2. ***Modernize Key Management Services***. Make key materials to set up secure information channels available over the network and easy to obtain and use. Integrate key order, generation, and distribution with other enterprise security services, reduce the logistics burden and security risk of key pre-placement, and enable networks to dynamically counter threats, and communities to organize at the speed of information.

2.2. **Manage Access**. Enable secure, authenticated access among users, services, data, platforms and facilities based on mission needs. In this context, access includes visibility, configuration, connection and allocation, as well as authorization for use.

2.2.1. ***Manage Identity Credentials***. Provide individuals and non-person entities (e.g., devices, applications, platforms) with credentials that allow them to authenticate their identities within an enterprise, for information transactions as well as access to DoD installations, facilities, weapons platforms and other resources, while ensuring interoperability with interagency and international partners.

2.2.2. ***Manage Privileges***. Provide modular, composable security services (e.g., policy management, authorization, and decision enforcement) that decouple access management from applications and enable security policies to be dynamically tailored to mission need.

2.2.3. ***Manage Resources***. Provide the ability to generate and manage standardized trusted descriptors (e.g., context, quality and condition, or characteristics) of resources, information, and services offered throughout the enterprise. This foundational activity (e.g., security attributes or metadata) will make cyber transactions, such as connecting devices to the network, configuring assets for new tasks, setting up COIs, and discovering information, easier, faster, and more reliable.

2.3. **Assure Information Sharing**. Enable secure, seamless information management and collaboration across information or security domains. Provide a full suite of secure sharing solutions for collaboration across networks, enclaves and COIs and with mission partners.

2.3.1. ***Assure Publishing***. Enable secure posting of information throughout the information enterprise based on dissemination controls, information tagging, provenance, and pedigree.

2.3.2. ***Assure Discovery***. Provide the ability to securely locate data, services, and users across the extended information enterprise.

2.3.3. ***Assure Collaboration***. Allow GIG users to seamlessly collaborate across information or security domains. Allow mission partners coming from organizations with different access-granting infrastructures to transparently collaborate with GIG users from their native information environments.

Goal 3. Anticipate and prevent successful attacks on data and networks

Rationale: The GIG is under constant attack. Attackers seek to steal Defense information and subvert command and control capabilities. To counter this, the Department will identify and stop attackers outside or at the perimeter whenever possible, but design and configure systems to ensure that attackers are easy to find and/or contain if they should pierce perimeter defenses. Traditional approaches have focused on reducing vulnerabilities instead of consequences; however, GIG perimeters are far-ranging and extensive hardening may result in reduced mission capability. Technologies that prevent unauthorized action are rapidly maturing. Incorporating them into the strategy provides some perimeter flexibility, helps ease maneuverability within the GIG by reducing the need for tough interior boundaries, and helps ease support for unanticipated missions and users. Further, it offers the advantage of secondary lines of defense should a perimeter be breached.

Outcomes:

- GIG defenses are aligned across the enterprise.
- Attacks are anticipated and stopped outside or at the perimeter whenever possible.
- Attackers are quickly identified and stopped should they get in, and penetrations do little damage.

Direction of Change:

From	To
Pre-placed passive protective mechanisms.	Counter adversary campaigns, and deny them network space and time.
Count on the perimeter to keep the adversary out.	Design defense zones into the network and manage with policy to dynamically cordon. Securely configure nodes and services. Actively monitor network activity and dynamically adapt defenses to changing threats.
Turn off compromised assets – if you can find them.	Logically separate assets and activity to reduce adversary awareness and options – and know the network.
Throw away compromised assets because they can't be cleaned.	Refresh regularly by design.

Table 5. Direction of Change Enabled by Goal 3

Strategy Elements:

3.1. **Understand the Battlespace**. Align and benefit from audit, sensor, forensic and incident management inputs across the extended enterprise.

3.1.1. ***Know the Adversary***. Data mine network sensors and IT vulnerability reports, direct observation and/or study of adversary behavior or other sources, in order to characterize adversary's intentions, methods, tools, and capabilities; then adjust defenses as needed.

3.1.2. ***Know the Network***. Know the physical and logical arrangement (map) and interconnections among network elements, especially the entry and exit points, the network security features and functions, and the network vulnerabilities. Integrate and analyze information from sensors, audit services, authorized network activity, help desk, incident management, or other sources to identify network events that require intervention.

3.1.3. ***Understand Cyber Effects***. Characterize the consequences of cyber events to the information enterprise and supported missions.

3.2. **Prevent and Delay Attackers from Getting in the GIG**. Apply knowledge of the network, vulnerabilities and adversaries to harden GIG entry and embrace tactics, techniques, and procedures that favor defenders.

3.2.1 ***Defend Perimeters***. Layer and strengthen network perimeters and internal security zones as a first line of defense. This includes controlling and filtering traffic at gateways, limiting network entry/exit points, and positioning externally shared information assets in perimeter subnets or Demilitarized Zones (DMZs).

3.2.2. ***Harden Hosts and Networks***. Securely configure applications and network devices so they offer the adversary no opportunity for unauthorized access. This includes establishing and enforcing security configurations for all cyber assets, tracking and eliminating software and hardware vulnerabilities as they are discovered, and stopping known malicious code.

3.2.3. ***Assess Network Defenses***. Test and tighten network defenses using Red Teams, Blue Teams and other mechanisms.

3.3. **Prevent Attackers from Staying in or Acting**. Lower the value of an attack for the attacker and reduce the consequences of an attack for the Department. Detect malicious activity through passive sensors and active investigation. Reconfigure assets to foil attackers. Implement mechanisms that limit what the attacker can see, where they can go, or what they can control.

3.3.1. ***Detect and Diagnose***. Find malicious behavior through passive and active monitoring and assess cause and effects.

3.3.2. ***Constrain Privileges***. Configure assets and processes to minimize what an attacker can do through methods such as least privilege, two-person administrative control, data-at-rest encryption, and application white-lists.

3.3.3. ***Eliminate Persistence***. Remove static cyber conditions that attackers depend on to remain in the network by adhering to proper configuration procedures, and frequently refreshing the system/network to a known good state, and technology.

3.3.4. ***Prevent Masquerading***. Prevent an attacker from using someone else's credentials by authenticating devices, users, services, and data sources for all cyber transactions. Prevent the attacker from monitoring for indicators such as credential use in concurrent locations/sessions or from unexpected or unusual locations.

3.3.5. ***Constrain Freedom of Movement***. Minimize where an attacker can go through techniques such as cordoning off portions of the network (to isolate attacks or protect the healthy), encrypting data at rest, and halting the unauthorized outbound communication or exfiltration of data**.**

Goal 4. Prepare for and operate through cyber degradation or attack

Rationale: Cyberspace resiliency (being flexible, adaptable, and successful in the face of cyber degradation, loss or attack) has three conditions: (1) cyber assets are trustworthy, (2) GIG-dependent missions are prepared, and (3) GIG operations have the means to prevail. Cyber assets are under constant stress and inevitably degrade over time. The remedy is to continuously monitor and repair. The magnitude of the GIG and the dynamics of defense missions demand that the GIG itself as well as the cyber assets that compose it be designed to self-monitor, self-attest, and self-repair. Because assets are globally sourced, assurance also includes knowing and having confidence in suppliers and service providers. Mission planners need to consider the full range of cyber situations and conditions, including loss of all cyber capabilities, and account for how the GIG will be operated and defended when degraded or under attack. This includes how GIG operations and defense may impact missions, and how missions can and should support GIG defensive operations. GIG operations and defense need to be appropriately staffed, equipped and integrated with other cyber operations across the extended enterprise.

Outcomes:

- Weapons systems, other defense platforms, and hosts and networks have assurance and survivability properties appropriate for use.
- Data and ICT components can measure and attest to their own trustworthiness.
- Response capabilities are integrated and readiness levels are sustained.
- GIG-dependent missions account for and respond effectively to the full range of cyber events and conditions.
- Enterprise capabilities recover quickly from damage.

Direction of Change:

From	To
IT efficiency.	Cyberspace resiliency.
Rely on system design and asset separation for integrity.	Use components with integrity checking built in (e.g., Trusted Platform Module (TPM), measurement, attestation). Monitor the behavior of globally sourced assets. Monitor DoD data for integrity over time. Use trusted sources augmented with system design and separation for critical assets.
Assume the network is impregnable.	Plan for operations to continue under all cyber situations and conditions. Ensure the GIG can recover quickly from damage.
Emergency response.	Cyber-aware mission planning and execution.

Table 6. Direction of Change Enabled by Goal 4

Strategy Elements:

4.1. **Develop and Maintain Trust in Data, Platforms, and Networks**. Guarantee the continued integrity and availability of cyber assets, to include processors and controllers embedded in weapons systems or other defense platforms.

4.1.1. ***Assure for Use***. Match supplier and product assurance to mission criticality and acquire products with assurance appropriate for use.

4.1.2. ***Engineer for Survivability***. Ensure networks and services identified as critical are engineered to operate despite sophisticated cyber attack.

4.1.3. ***Maintain Integrity***. Improve confidence that data and ICT components are sound at creation and remain so for as long as they are used.

4.2. **Strengthen Cybersecurity Readiness**.

4.2.1. ***Enable Cyber Event Response***. Link centers and operations across the extended enterprise and provide decision support for mission planning.

4.2.2. ***Exercise under Realistic Cyber Scenarios***. Test procedures and tactics for work arounds and fall-backs in the face of hostility. Conduct periodic exercises or evaluations of the ability to operate in a "cyber-out" environment; that is, one that assumes loss of all cyber assets and connectivity.

4.2.3. ***Identify Critical Cyber Assets***. Ensure a criterion exists for identifying cyber assets as critical and ensure assets meeting the criteria are so identified.

4.2.4. ***Improve Continuity Planning***. Determine how missions will continue in the face of degraded or unavailable cyber assets, and establish priorities for restoration.

4.3. **Sustain Missions**

4.3.1. ***Respond to Cyber Events***. Assess cyber damage and prepare and execute courses of action for 'fighting through' adverse cyber effects.

4.3.2. ***Sustain Mission Critical Functions under Degradation***. Dynamically allocate cyber resources as needed to sustain mission operations while addressing cyber failures, no matter the cause.

4.3.3. ***Reconstitute Critical Cyber Assets***. Rapidly restore cyber assets to a trusted state to support ongoing mission operations.

V. Implementation

Measuring progress, rebalancing and synchronizing capability investments to implement CIIA goals will be accomplished in coordination with capability portfolios. CIIA equities and investments are aligned primarily with the Net-Centric CPM, whose processes will be leveraged.

The next level of detail is classified and is located on the SIPRNet at http://www.intelink.sgov.gov/wiki/DoD_IETP/Priorities/Secured_Availability. This is an active site and its contents change over time. It includes detailed approaches and guidelines for each DoD CIIA Goal, as illustrated in Table 1 and the strategic capabilities illustrated in Table 2.

Appendix A – Acronyms

CIIA	Cyber, Identity and Information Assurance
COI	Community of Interest
CMS	Corporate Management and Support
CND	Computer Network Defense
CPM	Capability Portfolio Management
DAS	Defense Acquisition System
DIB	Defense Industrial Base
DISN	Defense Information Systems Network
DMZ	Demilitarized Zone
DNI	Director for National Intelligence
DNS	Domain Name Service
DOTMLPF	Doctrine, Organization, Training, Materiel, Leadership, Policy, Facilities
FA	Force Application
GIG	Global Information Grid
IA	Information Assurance
ICT	Information and Communications Technology
IE	Information Enterprise
IFF	Identification Friend or Foe
IM/IT	Information Management/Information Technology
JCA	Joint Capability Area
JCIDS	Joint Capabilities Integration Development System
NCO	Net-Centric Operations
NetOps	Network Operations
NIPRNet	Unclassified Internet Protocol Router Network
NMS-CO	National Military Strategy for Cyberspace Operations
OTNK	Over-the-Net Keying
PEO	Program Executive Office
PMO	Program Management Office
PPBE	Planning, Programming, Budgeting, and Execution
SCIF	Special Compartmented Information Facility
SIPRNet	Secret Internet Protocol Router Network
TPM	Trusted Platform Module
UAV	Unmanned Aerial Vehicle
UCDMO	Unified Cross Domain Management Office

Appendix B. Strategic Capabilities

The CIIA Strategy is lays out four goals for achieving the Department's vision for CIIA:

1. Organize for unity of purpose and speed of action.
2. Enable secure mission driven access to information and services.
3. Anticipate and prevent successful attacks on data and networks.
4. Prepare for and operate through cyber degradation or attack.

Over time, the activities within the four goals create a unified set of enterprise capabilities, described in ascending order below.

Capability 1. Transactional Protection

Granular end-to-end security controls for each information transaction in a variable trust environment

Historically, the authority for a system-high environment has defined the set of IA requirements for protecting the information residing in that environment. These IA requirements are usually determined based on the protection requirements for the highest level of information processed in that environment (e.g., high water mark standards). Within a system-high environment, a mix of controlled interfaces (e.g., cross domain solutions) and procedural controls are used to allow movement of information to and from other system-high environments. These controlled interfaces and procedural controls do not provide the flexibility to support seamless real-time information exchange and collaboration across security levels.

The Department's transition to a highly dynamic and interconnected IE includes a requirement to collaborate seamlessly and share information both within the Defense information enterprise and across the collection of federated U.S., Allied, coalition, and industry partner environments. Because users have varying levels of trust and their systems have varying levels of CIIA capabilities and trust, the Department cannot rely on a static, system high approach. Instead, a more dynamic transactional approach to CIIA is needed that determines whether a given information transaction should occur based on factors, such as the sensitivity (e.g., classification, perishability, releasability) of the information being exchanged, the mission's criticality (e.g., priority), and the ability of the systems supporting the transaction to sufficiently protect the information or service.

A transactional CIIA approach means information is protected end-to-end throughout its life cycle (i.e., during processing, storage, and transit), and it means traditional information access control mechanisms must be enhanced. The combination of end-to-end information protection and enhanced access control mechanisms ensures that information will only be shared when authorized and when the information can be sufficiently protected within the supporting information systems. This allows information to be broadly posted, discovered, and securely shared. Since the information transactions are independently protected in an end-to-end fashion, the need for physically separate system-high environments is reduced.

Additionally, the end-to-end protections associated with a transactional approach greatly reduce the consequences of successful unauthorized entry into the IE.

The variable levels of trust throughout the IE require that access control models consider:

- Trust level of entities requesting access to information and services within the IE. Each entity is assigned a set of privileges based on trust level and operational role within the IE (e.g., clearance, operational role, community of interest membership, citizenship). These privileges must be verifiable for a given transaction, and must be able to be changed over time as the entity's trust level or operational role changes.
- Access control and protection requirements for information and services residing within the IE. Each information object has an authority (e.g., the data provider, creator, or designated release authority) responsible for determining the access requirements and level of protection required for that object. The authority uses factors such as the information's classification, perishability, and releasability in determining the access and information protection requirements. These factors are derived from classification guides or other policies or procedures, and are specified within the information object's metadata.
- Physical environment into which the information is being released. Examples of this include a physically protected office environment [e.g., Special Compartmented Information Facility (SCIF)], a wireless mobile environment (e.g., "BlackBerry"), or coalition sovereign environment.
- Ability of transport systems [e.g., Defense Information Systems Network (DISN), Internet, foreign carrier] and the robustness of IA functionality within the users' workstations participating in the information transaction to sufficiently protect the information throughout its life cycle.
- User mission needs. For example, correlating a tactical user's location on the battlefield to coordinates of an Unmanned Aerial Vehicle's (UAV's) video feed to evaluate mission need.

Automated mechanisms can use these criteria to allow information to be shared during a given transaction based on the entity's trust level (i.e., privileges) and the end-to-end protection capabilities of the supporting information systems.

Capability 2. Cyber Identification Friend-or-Foe (Cyber IFF)

Universal cyber identification friend or foe (IFF) for all persons (individuals, roles, COIs, organizations) and all non-person entities (devices, platforms, data, services, systems, networks) in the GIG and its extensions to mission partners

Universal identities are fundamental. They enable every other strategic capability described in this Appendix and they provide for non-repudiation and improve attribution. There is no place for anonymous activities in net-centric operations. Potential improvements include:

- Extending the identity infrastructure to all GIG networks
- Stronger, multi-factor authentication for both persons and non-person entities
- Better protection against identity theft.

- Standard credentialing processes and improved (simpler and more reliable) ways to establish the identities of persons and non-person entities, including the use of authoritative attributes as appropriate.
- Improved acceptance of credentials for personnel from non-DoD organizations.
- Better separation of authentication and authorization.
- Improved forensics.
- Stronger integration with physical security systems.

Capability 3. Trusted Data and Platforms

Robust integrity mechanisms protecting Defense data and embedded within GIG and weapons system components and maintained over their life cycle

Regulating sharing based on how well information can be protected requires the distribution of CIIA functionality across the IT components that make up the IE. Achieving a needed level of integration, flexibility, and cost effectiveness requires greater use of commercially available products and greater reliance on software-based CIIA functionality. This means we must be confident that the computing platforms, to include embedded processors and controllers, perform correctly. Areas requiring greater assurance include:

- Mechanisms that protect information integrity and confidentiality during storage and processing. This includes user information as well as the computing platform's configuration information.
- Mechanisms that segregate information at varying levels of sensitivity within a computing platform. Examples of this include segregating information between users who share a system, segregating computing platform configuration information from users of the system, and segregating information that is being processed simultaneously on a single platform (e.g., concurrent single level and multi-level operation).
- Mechanisms that enable computing platforms to protect themselves from network-based attacks (e.g., malicious code, viruses, spyware), especially in the broader, interconnected federated environment. Key to this is ensuring that the hardware and software performing CIIA functions are properly configured during installation and remain so throughout their life cycle.
- Mechanisms that ensure hardware and software are robust enough for the intended use -- design, evaluation, testing, and certification processes (i.e., hardware and software assurance).
- Mechanisms that protect against supply chain risk.

Integrity and trust in the information and the services operating within the IE are easily lost and, once lost, can be difficult to regain. Because of this, CIIA considerations must be applied across the spectrum of how the information enterprise is procured; "used" to accomplish mission objectives; "maintained" to protect against atrophy in either capability or assurance; and "evolved" to meet dynamic mission needs and increasing cyber threats. Failure to fully address CIIA life cycle management may enable an adversary to obtain the design, configuration, and implementation details necessary to plan, access and modify the hardware and/or software components which, in turn, enables the adversary to alter the performance of a weapons system or gain/deny access to an information system.

Assurance levels and practices should be based on the criticality of an ICT component to meeting mission objectives. For instance, components that support protection of more sensitive information or provide service to missions with greater availability requirements require a more stringent life cycle management approach to ensure that those components are sufficiently trustworthy. How and where components are developed, manufactured, purchased, tested, integrated into the IE, configured, operated, and maintained are critical aspects of the life cycle management of CIIA and integral to the transactional IA approach that must assess whether or not to share information based on how well the components involved in the transaction can protect the information.

CIIA life cycle management practices must be better incorporated into the Department's larger decision processes (i.e., JCIDS, PPBE, and DAS), governance, and workforce development to ensure risks are appropriately considered. Ideally, each aspect of a component's life cycle management can be quantified to establish the level of trust used to support access control decisions, to include:

- "Pedigree" of a piece of equipment – who designed it, where was it built, and how it was obtained
- "Pedigree" of a system's life cycle – who installed it and maintains it and how is its security parameters configured (e.g., best commercial practices, DoD configuration guide, federal configuration guide)
- Trust level of the entity that maintains the configuration (e.g., industry or cleared contractor/government personnel)
- How well the system ensures that its configuration is correct, e.g., are software downloads limited to authorized sources and are integrity mechanisms applied, is the configuration frequently checked and refreshed from known good source, are physical security audits performed, and are inventory controls utilized?

Integrity and trust considerations also exist at the enterprise. Sound network underpinnings are essential, e.g., Domain Name Service (DNS) and router security, resolution of security issues associated with networking protocol migrations (e.g., IPv6), and protection of network addresses against unauthorized or unnecessary exposure. Diversity in the types, placement, configuration, robustness, and suppliers of protection mechanisms utilized by an environment can improve protection effectiveness, increase the likelihood of detecting inappropriate activity, increase time and cost for an attacker (thus reducing attack likelihood), and reduce the consequences of an adverse cyber event.

Capability 4. Cyber Surveillance and Reconnaissance

Technologies and processes to persistently observe GIG user, asset, and network behavior and examine their characteristics or configuration to detect anomalies, misuse, or unauthorized activity

Broader information sharing, unanticipated users, greater interconnectivity of systems, and employment of globally sourced ICT, requires enhanced monitoring, misuse detection, and robust capabilities to prevent sophisticated adversaries from gaining insider access. This includes:

- Approaches to limit the ability of an outsider to gain understanding of the environment's internal configuration (including configuring protection mechanisms within the environment) that could be used to identify avenues of attack.
- Mechanisms to limit the ability to alter an environment's system configuration to enable unauthorized entry; or, in the case where a user has been provided some level of legitimate access (e.g., maintenance personnel, coalition partner), to prevent escalation of privileges or level of access.
- Mechanisms to significantly increase the probability of being detected and identified and increase the cost and difficulty of taking unauthorized action. This includes mechanisms to limit the ability to freely access and exfiltrate information contained within the environment.

A distributed sensor grid supports the ability to audit, monitor, search for, track, and contain unauthorized activity and misuse, and monitor the perimeter (e.g., Internet, sovereign network, and tactical system boundaries). The distributed sensor grid, coupled with enhanced transactional IA access control mechanisms, enables tracking of user actions within the information enterprise to detect misuse and insider activities. The distributed sensor grid includes special purpose sensors; CIIA devices (e.g., firewalls, intrusion detection systems, cross domain solutions, and transactional access control mechanisms) and any component or device that touches a network (e.g., clients, servers, and routers).

Inputs from the distributed sensor grid can be collected across classification levels, missions, and COIs, allowing monitoring and analysis to occur throughout the extended IE. In addition to maintaining pervasive CIIA situational awareness, operators can actively search for, find and respond to events within the enterprise. A dynamic response capability, based on tailorable digital policy, enables an event response to be coordinated and de-conflicted across the IE. It also allows the mission impact of the event response to be assessed, possibly resulting in updated digital policies being generated and distributed that will contain the event or implement other response actions.

Capability 5. Enterprise Security Management

Integrated enterprise services for all security functions (e.g., identity, credential, attribute, policy, privilege, authentication, configuration, audit, and cryptologic key management)

The information enterprise will continue to be a high priority target under attack by adversaries with a wide range of skill levels and motivations, and the impact of system outages, degradations, cyber attacks, and contention for limited resources within dynamic tactical environments will likely continue to expand. Increased interdependence and interconnection of systems will affect ability to contain these impacts and increase the attack avenues available to adversaries. Implementing policy-based management (PBM) throughout the enterprise allows dynamic, highly automated, coordinated establishment and enforcement of information access, communities of interest, mission priorities, resource allocations (including bandwidth and connectivity), and responses to cyber attack. This capability enables resources to be adjusted to ensure that the highest priority missions continue to receive resources needed for mission success, while at the same time limiting attack paths into the IE. This can slow the spread of attacks to neighboring systems and block avenues that could be used to exfiltrate information from the IE. Key aspects are:

- Ability to coordinate and de-conflict digital policy at the local, regional, and enterprise levels to ensure that policy updates do not impact mission operations in unintended ways.
- Ability to distribute and enforce the digital policy consistently across the collection of interdependent information systems and net-centric services.
- Ability to automatically assess compliance with distributed digital policy.
- Ability to coordinate and leverage all security functions for a given objective.

Nine key services comprise enterprise security management: identity, credential, attribute, policy, privilege, authentication, configuration, audit, and cryptologic key management.

Integration of all security management services enables consistent control of the security aspects of the IE, reduces operational burden and configuration errors, improves real-time support for dynamic changes, and minimizes dependence on users and system administrators to understand and enforce cyber security.

Capability 6. Dynamic Defense

Enterprise security management infrastructure linked to and alerted by extended cyber sensor networks

See http://www.intelink.sgov.gov/wiki/DoD_IETP/Priorities/Secured_Availability for more discussion.

Capability 7. Mission-based Architecture

Networks, services, and data organized and optimized for mission availability

Current GIG network segmentation (e.g., NIPRNet, SIPRNet) is driven by information confidentiality needs, not by mission needs. The primary mission drivers are availability and integrity. As reliance on network segmentation for confidentiality diminishes through realization of the strategic capabilities described above, missions and information enterprise need to be co-designed to reduce the mission consequences of adverse cyber events. This includes the ability to:

- Securely realize the promise of platforms, software, and infrastructure as services (i.e., “cloud computing”) and evolving software development and design methods (i.e. “Web 2.0/3.0”)

- Separate less critical missions or functions from more critical ones, and more risky services from those less risky.
- Define and implement a range of integrity and availability service performance requirements and metrics with criteria for assignment to differing mission scenarios, to include high availability requirements in austere, band-width constrained environments.
- Dynamically [re]allocate resources based on changing mission needs or changing cyber asset availability.
- Deploy segregated "acceptable trust" platforms or computing/access methods, e.g., for persons teleworking or in transit.
- Pre-engineer and pre-position options for users to adjust security levels in response to changing mission needs.
- Conduct status monitoring.
- Conduct fine grained data integrity monitoring.
- Rapidly reconstitute assets to a known good state, especially data.

DASD Cyber, Identity and Information Assurance